# PRBIT - Princípy bezpečnosti informačných technológií

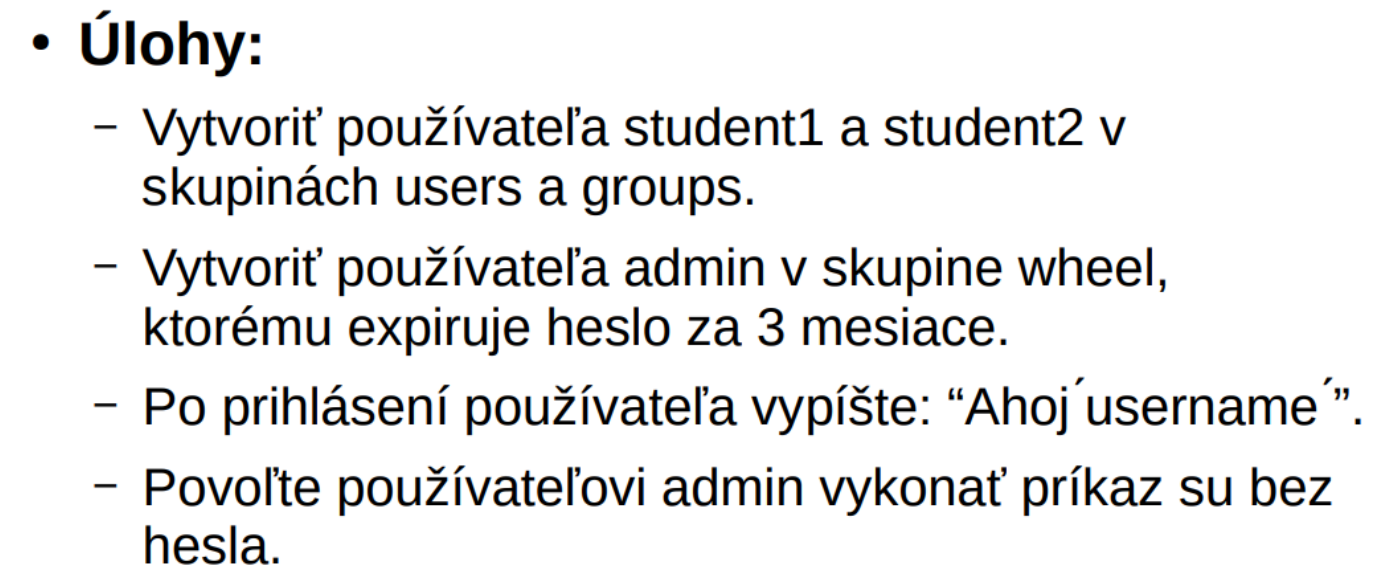
## Report - Domáca úloha č.1

Autor: Marek Čederle

Cvičenie: Pondelok 17:00

### Použité príkazy a ich vysvetlenie

Zadanie č.1




```
sudo groupadd wheel users groups
sudo useradd --groups users,groups student1
sudo useradd --groups users,groups student2
sudo useradd --group wheel admin
sudo chage --maxdays 90 admin
```

- `groupadd` - príkaz na vytvorenie skupiny (parametre su názvy skupín)
- `useradd` - príkaz na vytvorenie používateľa
  - `--groups` - prepínač, ktorý pridá používateľa do skupín (parametre sú názvy skupín, syntax je dôležitý a treba nemať medzery)
  - `student1` - názov používateľa
- `chage` - príkaz na zmenu nastavení používateľského účtu a vypršania jeho hesla
  - `--maxdays` - prepínač, ktorý nastavuje maximálny počet dní, po ktorých vyprší heslo (s parametrom `90` - počet dní)
  - `admin` - názov používateľa

Treba vytvoriť hociaký súbor v `/etc/profile.d`, môj má názov `welcome_message.sh`:

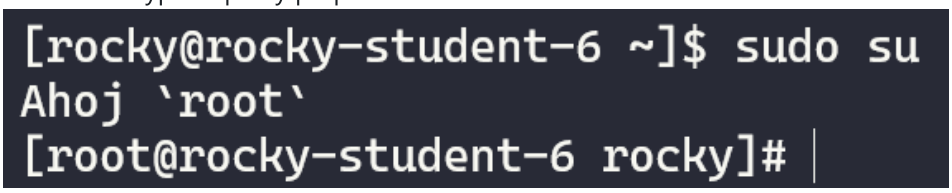
```
sudo nano /etc/profile.d/welcome_message.sh
```

Následne do neho pridať tento kód a uložiť ho:

```
#! /bin/bash
echo "Ahoj \`$(whoami)\`"
```

- `#! /bin/bash` - shebang, ktorý hovorí, že sa jedná o bash skript
- `echo` - príkaz na výpis textu
- `$(whoami)` - príkaz, ktorý vráti názov používateľa, ktorý je prihlásený

Testovanie výpisu správy pri prihlásení:




Spustenie bezpečného editora pre súbor `/etc/sudoers`:

```
sudo visudo
```

Treba pridať do súboru `/etc/sudoers` (optimálne na koniec) nasledovný riadok:

```
admin   ALL=(ALL)   NOPASSWD: /bin/su
```

- `admin` - názov používateľa
- `ALL` - platí to pre všetkých hostov
- `NOPASSWD` - znamená, že sa nemusí zadávať heslo pri príkaze `su`

Testovanie použitia príkazu `su` bez hesla na používateľovi `admin`:

```
[student1@rocky-student-6 rocky]$ su rocky
Password:
[student1@rocky-student-6 rocky]$ sudo su rocky

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for student1:
sudo: a password is required
[student1@rocky-student-6 rocky]$ exit
exit
[admin@rocky-student-6 rocky]$ whoami
admin
[admin@rocky-student-6 rocky]$ sudo su student1
Ahoj `student1`
[student1@rocky-student-6 rocky]$
```

Zadanie č.2

- **Úlohy:**
  - Zaraďte používateľa student1 do skupiny studenti.
  - Nastavte limit na maximálnu veľkosť súboru 300 kB pre skupinu studenti.
  - Nastavte politiku hesiel na:
    - minimálne 4 číslice,
    - dĺžka aspoň 10 znakov,
    - heslo rozdielne v 3 znakoch od posledného.

Keďže používateľ `student1` už bol vytvorený, tak ho treba iba modifikovať, načo slúži príkaz `usermod`.

```
sudo usermod -aG studenti student1
```

- `-a` - (append) pridá používateľa do skupiny (nemažú sa ostatné skupiny)
- `-G` - (group) hovorí o tom že sa ide používateľ pridať do skupiny
- `studenti` - skupina do ktorej sa pridáva používateľ
- `student1` - používateľ, ktorý sa pridáva do skupiny

Na koniec súboru `/etc/security/limits.conf` treba pridať riadok:

```
@studenti    hard    fsize    300
```

- `@studenti` - @ je použitý pre označenie skupiny (studenti je názov skupiny)
- `hard` - nastavuje hard limit (nemôže ho používateľ zmeniť ani prekročiť)
- `fsize` - parameter ktorý hovorí o limite na veľkosť súboru
- `300` - veľkosť súboru v kB (kilo-bytoch)

Testovanie veľkosti súboru:

```
[student1@rocky-student-6 test]$ cat test.txt >> test2.txt
[student1@rocky-student-6 test]$ cat test.txt >> test2.txt
[student1@rocky-student-6 test]$ cat test.txt >> test2.txt
[student1@rocky-student-6 test]$ cat test.txt >> test2.txt
[student1@rocky-student-6 test]$ cat test.txt >> test2.txt
[student1@rocky-student-6 test]$ cat test.txt >> test2.txt
[student1@rocky-student-6 test]$ ls -alh1
total 140K
drwxr-xr-x. 2 student1 studenti  39 Sep 17 12:16 .
drwx------. 3 student1 studenti  95 Sep 17 12:15 ..
-rw-r--r--. 1 student1 studenti 94K Sep 17 12:17 test2.txt
-rw-r--r--. 1 student1 studenti 11K Sep 17 12:16 test.txt
[student1@rocky-student-6 test]$ cat test2.txt >> test.txt
[student1@rocky-student-6 test]$ cat test2.txt >> test.txt
[student1@rocky-student-6 test]$ cat test2.txt >> test.txt
[student1@rocky-student-6 test]$ ls -alh1
total 448K
drwxr-xr-x. 2 student1 studenti   39 Sep 17 12:16 .
drwx------. 3 student1 studenti   95 Sep 17 12:15 ..
-rw-r--r--. 1 student1 studenti  94K Sep 17 12:17 test2.txt
-rw-r--r--. 1 student1 studenti 290K Sep 17 12:17 test.txt
[student1@rocky-student-6 test]$ cat test2.txt >> test.txt
File size limit exceeded (core dumped)
[student1@rocky-student-6 test]$ ls -alh1
total 448K
drwxr-xr-x. 2 student1 studenti   39 Sep 17 12:16 .
drwx------. 3 student1 studenti   95 Sep 17 12:15 ..
-rw-r--r--. 1 student1 studenti  94K Sep 17 12:17 test2.txt
-rw-r--r--. 1 student1 studenti 300K Sep 17 12:17 test.txt
[student1@rocky-student-6 test]$
```

Do súboru `/etc/security/pwquality.conf` treba pridať riadky:

```
difok = 3
minlen = 10
dcredit = -4
```

- `difok` - počet znakov, ktoré sa musia líšiť od predchádzajúceho hesla
- `minlen` - minimálna dĺžka hesla
- `dcredit` - minimálny počet číslic v hesle (mínus značí že ide o minimálny počet, bez znamienka by to bolo maximálny počet)

Testovanie zmeny hesla:

```
[student1@rocky-student-6 rocky]$ passwd
Changing password for user student1.
Current password:
Current Password:
passwd: Authentication token manipulation error
[student1@rocky-student-6 rocky]$ passwd
Changing password for user student1.
Current password:
New password:
BAD PASSWORD: The password contains less than 4 digits
passwd: Authentication token manipulation error
[student1@rocky-student-6 rocky]$ passwd
Changing password for user student1.
Current password:
New password:
BAD PASSWORD: The password is shorter than 10 characters
passwd: Authentication token manipulation error
[student1@rocky-student-6 rocky]$ passwd
Changing password for user student1.
Current password:
New password:
BAD PASSWORD: The password is too similar to the old one
passwd: Authentication token manipulation error
[student1@rocky-student-6 rocky]$
```